IntraVUE Diagnostics

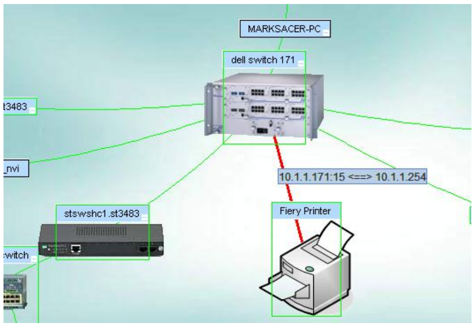
IntraVUE provides a method to record and capture the issues that occur in the Ethernet networks being used for automation applications. Automation networks are susceptible to subtle disturbances due to the real time nature of the applications, as well as the timing requirements of the connected equipment. Environmentally created problems, as well as “cause and effect” actions can create intermittent disturbances that will be hard to detect by conventional networking tools.

Although IntraVUE can provide an accurate assessment of the connected devices and their interconnections, it is the ability to sense problems on the network that provides the greatest value. IntraVUE has helped quickly identify many common problems in these automation networks. The following covers the variety of issues identified by IntraVUE and how they are represented. These include:

1. Device failure
2. Duplicate IP Address
3. Broadcast or Multicast Storm
4. Intermittent Connection problems
5. Devices accidentally moved
6. Foreign computers momentarily linking to the network
7. Large File transfers between devices
8. Bad RSTP, Ring Switches, or accidental cable loops
9. Resetting Switch
10. Overloaded or misbehaving devices

Device Failure

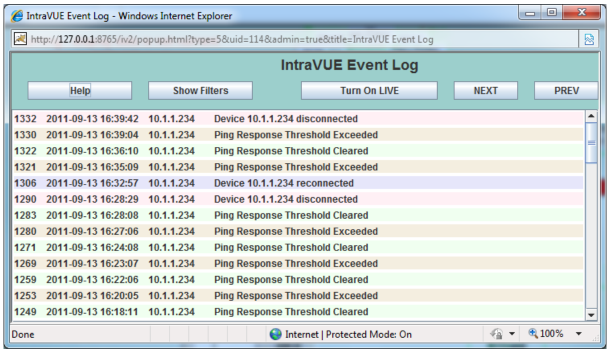
Device failures are common in any system. The key issue in an automation system is getting the failed device back up and running. This is especially important if the device has shut down a production line. The typical first responders are technicians who understand the devices but who may not have a great deal of network experience. It is thus important to provide the details so that the device can be reset or replaced.



IntraVUE provides a live animated graphic that can show a disconnected device by a red line. Hovering over the line will provide details as to the port on the switch the device is connected. See the picture to the left.

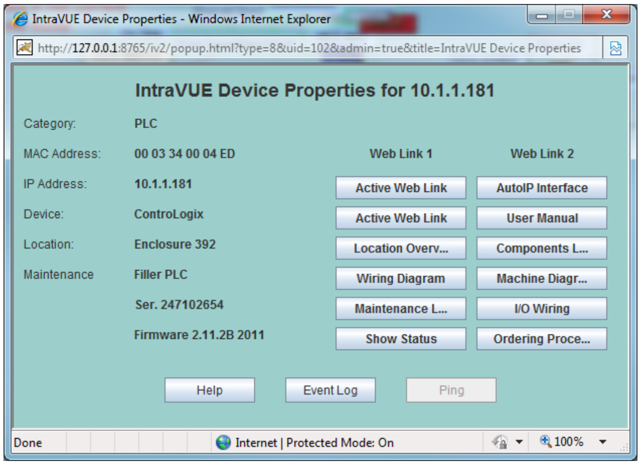
A first check would be to see if the connection to the switch is still made. Many times a disconnected device may be as simple as a connector dislodged as someone works on the switch.

Additional details can be obtained on the time of the disconnection and if there have been several intermittent disconnections prior to the failure by opening up the event log. This information can be easily achieved by right clicking on the device and bringing up the event log for the device. The event log will contain a


IntraVUE Event Log - Windows Internet Explorer
http://127.0.0.1:8765/iv2/popup.html?type=5&uid=114&admin=true&title=IntraVUE Event Log
IntraVUE Event Log
Help
Show Filters
Turn On LIVE
NEXT
PREV
Done
Internet | Protected Mode: On
100%

```
1332  2011-09-13 16:39:42  10.1.1.234   Device 10.1.1.234 disconnected
1330  2011-09-13 16:39:04  10.1.1.234   Ping Response Threshold Exceeded
1322  2011-09-13 16:36:10  10.1.1.234   Ping Response Threshold Cleared
1321  2011-09-13 16:35:09  10.1.1.234   Ping Response Threshold Exceeded
1306  2011-09-13 16:32:57  10.1.1.234   Device 10.1.1.234 reconnected
1290  2011-09-13 16:28:29  10.1.1.234   Device 10.1.1.234 disconnected
1283  2011-09-13 16:28:08  10.1.1.234   Ping Response Threshold Cleared
1280  2011-09-13 16:27:06  10.1.1.234   Ping Response Threshold Exceeded
1271  2011-09-13 16:24:08  10.1.1.234   Ping Response Threshold Cleared
1269  2011-09-13 16:23:07  10.1.1.234   Ping Response Threshold Exceeded
1259  2011-09-13 16:22:06  10.1.1.234   Ping Response Threshold Cleared
1253  2011-09-13 16:20:05  10.1.1.234   Ping Response Threshold Exceeded
1249  2011-09-13 16:18:11  10.1.1.234   Ping Response Threshold Cleared
```

time based history of the device. The history can cover many months and thus if there are repeated issues they can be reviewed.



IntraVUE Device Properties for 10.1.1.181

Category:	PLC
MAC Address:	00 03 34 00 04 ED
IP Address:	10.1.1.181
Device:	ControLogix
Location:	Enclosure 392
Maintenance	Filler PLC
	Ser. 247102654
	Firmware 2.11.2B 2011

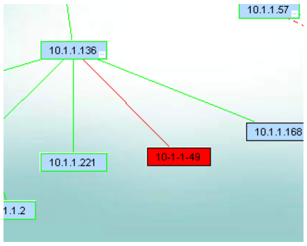
To obtain additional details for the affected device such as a maintenance log, user manual or other repair procedures one can click on the properties of the device.

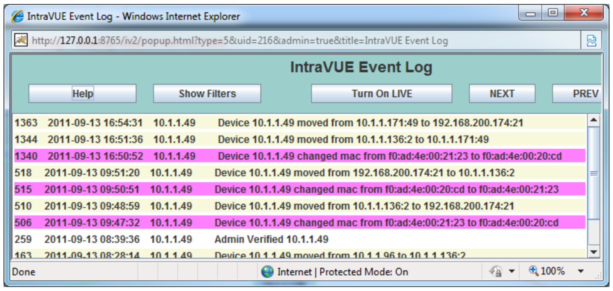
The Properties window can provide the IP address and MAC address of the device as well as Vendor and Model. Since IntraVUE is a Web Server this data is available to any computer that can browse to the IntraVUE system. It provides both technicians and Control engineers a common tool to quickly resolve basic problems.

Duplicate IP Address

Most devices in an automation network will have static addresses. Since for the most part assigning an IP address to a device is a manual process, the chances of a device getting an address that is in conflict rises as the number of devices increase. Duplicate addresses can create a great number of issues and should be avoided. It is thus important to quickly identify if a duplicate address has been added on your network.

IntraVUE can help quickly identify a duplicate address by tracking the IP, MAC and location of all devices on the network.



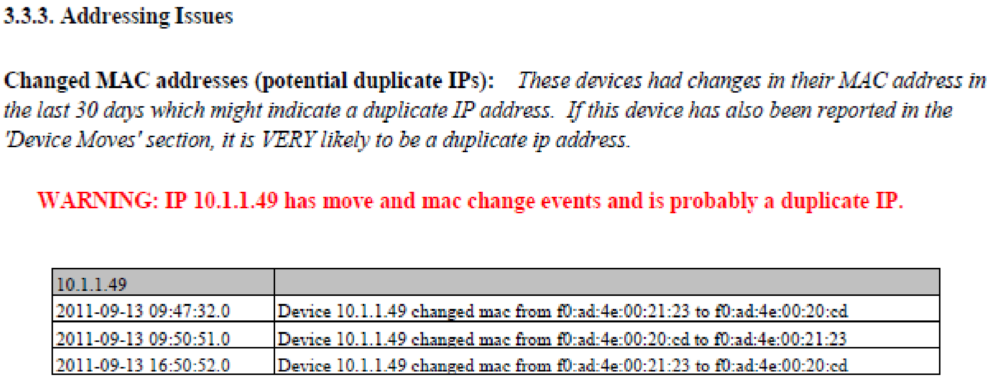

IntraVUE Event Log - Windows Internet Explorer
http://127.0.0.1:8765/iv2/popup.html?type=5&uid=216&admin=true&title=IntraVUE Event Log
IntraVUE Event Log
Help
Show Filters
Turn On LIVE
NEXT
PREV
Done
Internet | Protected Mode: On
100%

```
1363   2011-09-13 16:54:31   10.1.1.49    Device 10.1.1.49 moved from 10.1.1.171:49 to 192.168.200.174:21
1344   2011-09-13 16:51:36   10.1.1.49    Device 10.1.1.49 moved from 10.1.1.136:2 to 10.1.1.171:49
1340   2011-09-13 16:50:52   10.1.1.49    Device 10.1.1.49 changed mac from f0:ad:4e:00:21:23 to f0:ad:4e:00:20:cd
518    2011-09-13 09:51:20   10.1.1.49    Device 10.1.1.49 moved from 192.168.200.174:21 to 10.1.1.136:2
515    2011-09-13 09:50:51   10.1.1.49    Device 10.1.1.49 changed mac from f0:ad:4e:00:20:cd to f0:ad:4e:00:21:23
510    2011-09-13 09:48:59   10.1.1.49    Device 10.1.1.49 moved from 10.1.1.136:2 to 192.168.200.174:21
506    2011-09-13 09:47:32   10.1.1.49    Device 10.1.1.49 changed mac from f0:ad:4e:00:21:23 to f0:ad:4e:00:20:cd
259    2011-09-13 08:39:36   10.1.1.49    Admin Verified 10.1.1.49
163    2011-09-13 08:28:14   10.1.1.49    Device 10.1.1.49 moved from 10.1.1.96 to 10.1.1.136:2
```

IntraVUE will mark an IP address that appears in two locations with a red box as seen above. By selecting the event log you will see the two MAC addresses listed for an IP Address. This provides details of not only a duplicate address but the location of both devices and the time the conflict was first reported.

This information is also presented in the Diagnostic Report. The report will use the data collected and by determining that an IP address is switching between two MAC address as well as changing locations in the network. The Diagnostic Report will create a red text to easily identify a duplicate address. See below:

IntraVUE Diagnostics



3.3.3. Addressing Issues

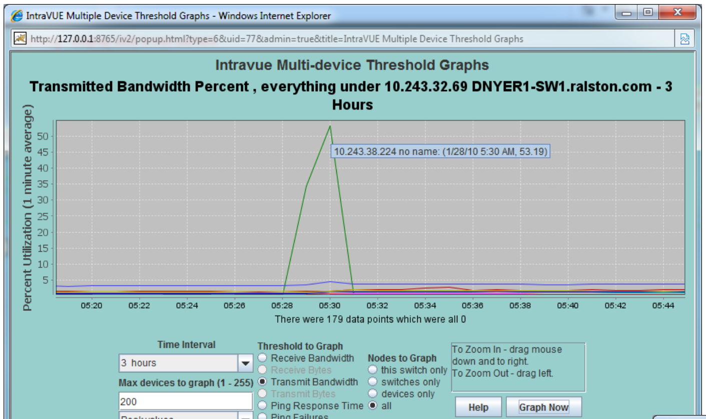
Changed MAC addresses (potential duplicate IPs): *These devices had changes in their MAC address in the last 30 days which might indicate a duplicate IP address. If this device has also been reported in the 'Device Moves' section, it is VERY likely to be a duplicate ip address.*

WARNING: IP 10.1.1.49 has move and mac change events and is probably a duplicate IP.

10.1.1.49	
2011-09-13 09:47:32.0	Device 10.1.1.49 changed mac from f0:ad:4e:00:21:23 to f0:ad:4e:00:20:cd
2011-09-13 09:50:51.0	Device 10.1.1.49 changed mac from f0:ad:4e:00:20:cd to f0:ad:4e:00:21:23
2011-09-13 16:50:52.0	Device 10.1.1.49 changed mac from f0:ad:4e:00:21:23 to f0:ad:4e:00:20:cd

Broadcast or Multicast Storm

At some times a device may generate a burst of broadcast or multicast traffic which will be received by many devices. The transmitted data may only last a short period of time and thus can be hard to find if not continually scanning for the occurrence. IntraVUE records and stores all of the transmitted and received levels on a minute basis and this recorded data can be used to determine not only the sources but also what devices may have received the bust. Using the Threshold Graphing feature one can choose to view all devices transmitting over time. In this graph you can see a single device generating a burst of traffic that exceeds 50% of the available bandwidth.



IntraVUE Multiple Device Threshold Graphs - Windows Internet Explorer

http://127.0.0.1:8765/iv2/popup.html?type=6&uid=77&admin=true&title=IntraVUE Multiple Device Threshold Graphs

Intravue Multi-device Threshold Graphs

Transmitted Bandwidth Percent , everything under 10.243.32.69 DNYER1-SW1.ralston.com - 3 Hours

10.243.38.224 no name: (1/28/10 5:30 AM, 53.19)

There were 179 data points which were all 0

Time Interval: 3 hours

Max devices to graph (1 - 255): 200

Peak values

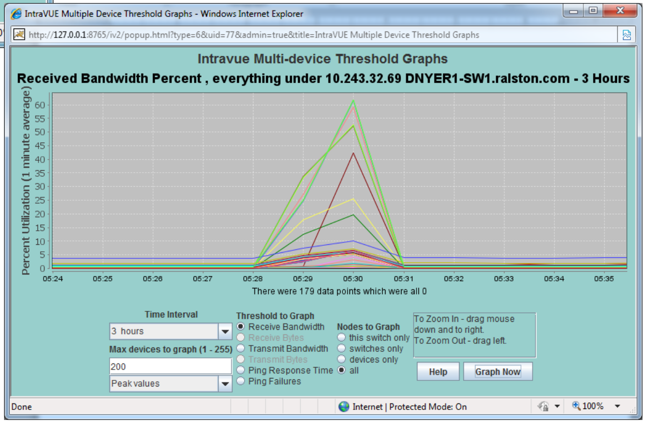
Threshold to Graph
○ Receive Bandwidth
○ Receive Bytes
● Transmit Bandwidth
○ Transmit Bytes
○ Ping Response Time
○ Ping Failures

Nodes to Graph
○ this switch only
○ switches only
○ devices only
● all

To Zoom In - drag mouse down and to right.
To Zoom Out - drag left.

Transmitted data graph clearly shows IP and time

In the next graph now listing Received Traffic you can see a group of devices that have been affected by the transmission. The data used in this example is from an actual customer application.



IntraVUE Multiple Device Threshold Graphs - Windows Internet Explorer

http://127.0.0.1:8765/iv2/popup.html?type=6&uid=77&admin=true&title=IntraVUE Multiple Device Threshold Graphs

Intravue Multi-device Threshold Graphs

Received Bandwidth Percent , everything under 10.243.32.69 DNYER1-SW1.ralston.com - 3 Hours

There were 179 data points which were all 0

Time Interval: 3 hours

Max devices to graph (1 - 255): 200

Peak values

Threshold to Graph
● Receive Bandwidth
○ Receive Bytes
○ Transmit Bandwidth
○ Transmit Bytes
○ Ping Response Time
○ Ping Failures

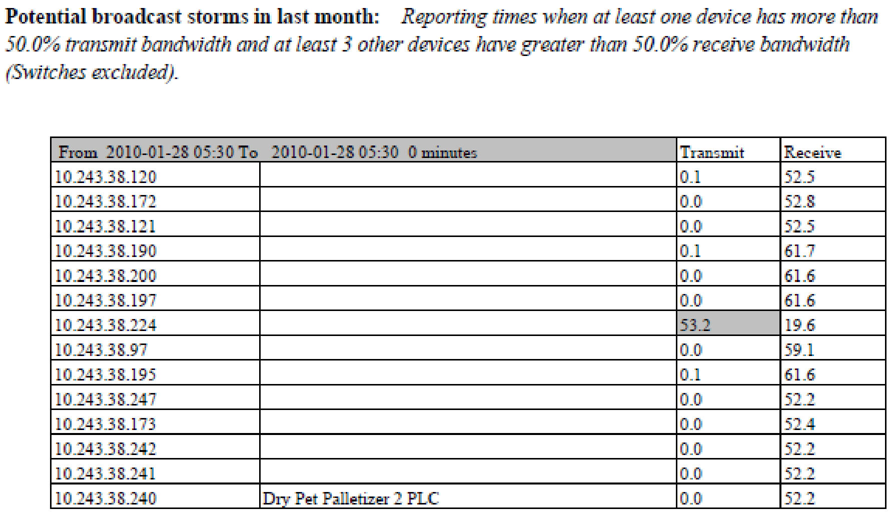
Nodes to Graph
○ this switch only
○ switches only
○ devices only
● all

To Zoom In - drag mouse down and to right.
To Zoom Out - drag left.

Received data affecting many devices on the network

If one were to use the Diagnostic Reporting system the data would have been presented in a table in which the IP addresses of all the affected equipment would be identified.

IntraVUE Diagnostics

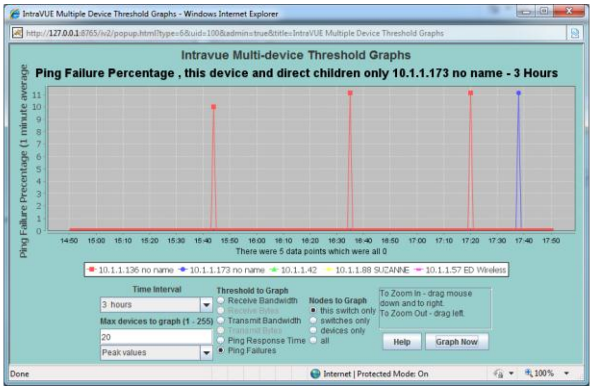


Potential broadcast storms in last month: *Reporting times when at least one device has more than 50.0% transmit bandwidth and at least 3 other devices have greater than 50.0% receive bandwidth (Switches excluded).*

From 2010-01-28 05:30 To 2010-01-28 05:30 0 minutes		Transmit	Receive
10.243.38.120		0.1	52.5
10.243.38.172		0.0	52.8
10.243.38.121		0.0	52.5
10.243.38.190		0.1	61.7
10.243.38.200		0.0	61.6
10.243.38.197		0.0	61.6
10.243.38.224		53.2	19.6
10.243.38.97		0.0	59.1
10.243.38.195		0.1	61.6
10.243.38.247		0.0	52.2
10.243.38.173		0.0	52.4
10.243.38.242		0.0	52.2
10.243.38.241		0.0	52.2
10.243.38.240	Dry Pet Palletizer 2 PLC	0.0	52.2

Intermittent Connection problems

Based on the environment which may contain vibration, electrical noise, and moisture many industrial devices can experience intermitted connection problems. IntraVUE continuously pings all the devices that have been found on the network between 8 and 12 times a minute. Each minute the results are compiled in a percent % failure rate per minute and stored in IntraVUE. In a good network there should be no ping failures.


IntraVUE Multiple Device Threshold Graphs - Windows Internet Explorer
http://127.0.0.1:8765/iv2/popup.html?type=6&uid=100&admin=true&title=IntraVUE Multiple Device Threshold Graphs
Intravue Multi-device Threshold Graphs
Ping Failure Percentage , this device and direct children only 10.1.1.173 no name - 3 Hours
Ping Failure Precentage (1 minute average
0
1
2
3
4
5
6
7
8
9
10
11
14:50
15:00
15:10
15:20
15:30
15:40
15:50
16:00
16:10
16:20
16:30
16:40
16:50
17:00
17:10
17:20
17:30
17:40
17:50
There were 5 data points which were all 0
10.1.1.136 no name
10.1.1.173 no name
10.1.1.42
10.1.1.88 SUZANNE
10.1.1.57 ED Wireless
Help
Graph Now
Done
Internet | Protected Mode: On
100%

Time Interval: 3 hours

Max devices to graph (1 - 255): 20

Peak values

Threshold to Graph: ○ Receive Bandwidth ○ Receive Bytes ○ Transmit Bandwidth ○ Transmit Bytes ○ Ping Response Time ● Ping Failures

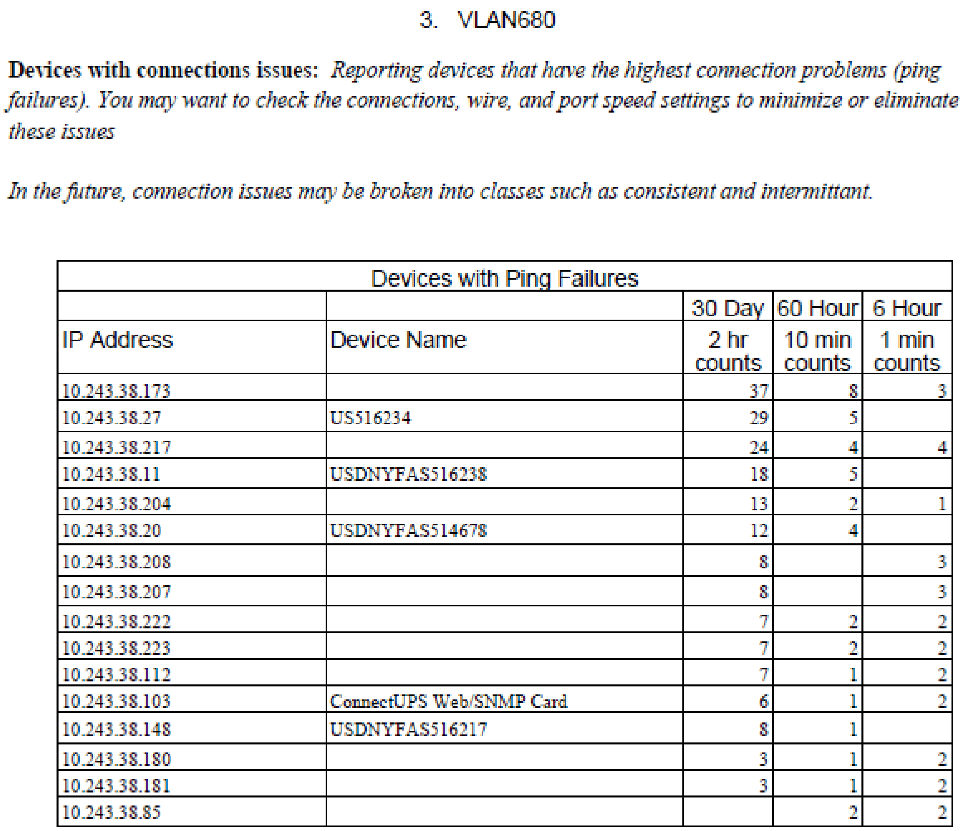
Nodes to Graph: ● this switch only ○ switches only ○ devices only ○ all

To Zoom In - drag mouse down and to right. To Zoom Out - drag left.

Ping failure percentages can be trended in a graphed to identify if there are connection problems. These graphs can help pinpoint the time and frequency of failures that help identify the potential causes. These can be created from environmental issues such as vibration or electrical noise from a large motor or a switch performing auto-negotiation based on a poor link. It can also display if a group of devices are affected at the same time which can point to a specific event or cause.

Time based view of Ping Failures

The diagnostic report will list the devices with the highest connection problems. The list will contain the failures that have occurred over the last 6 hours, 60 hours and 30 days to determine if the faults are recent.



3. VLAN680

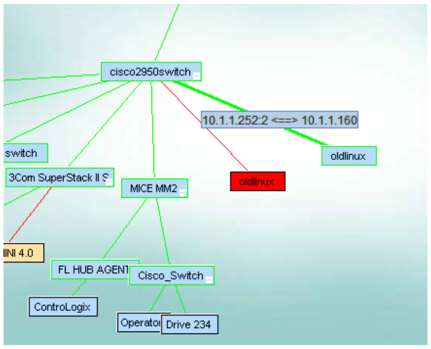
Devices with connections issues: *Reporting devices that have the highest connection problems (ping failures). You may want to check the connections, wire, and port speed settings to minimize or eliminate these issues*

In the future, connection issues may be broken into classes such as consistent and intermittant.

Devices with Ping Failures				
		30 Day	60 Hour	6 Hour
IP Address	Device Name	2 hr counts	10 min counts	1 min counts
10.243.38.173		37	8	3
10.243.38.27	US516234	29	5	
10.243.38.217		24	4	4
10.243.38.11	USDNYFAS516238	18	5	
10.243.38.204		13	2	1
10.243.38.20	USDNYFAS514678	12	4	
10.243.38.208		8		3
10.243.38.207		8		3
10.243.38.222		7	2	2
10.243.38.223		7	2	2
10.243.38.112		7	1	2
10.243.38.103	ConnectUPS Web/SNMP Card	6	1	2
10.243.38.148	USDNYFAS516217	8	1	
10.243.38.180		3	1	2
10.243.38.181		3	1	2
10.243.38.85			2	2

Devices accidentally moved

Many devices in an automation network are fixed to a specific port of a switch. In many cases the port is configured with a speed and duplicity that matches the unique requirements of the device. In other applications the port may be assigned to a specific VLAN. Many of these switches are located in electrical enclosures and additional devices are added frequently. The potential for a connection to be accidentally changed due to device additions or just servicing the switch is becoming more common. In other cases we have seen equipment such as Printers/labelers moved to another line, which have created other issues when the original line is started and that equipment is expected to be there. Keeping track of equipment can be challenging.

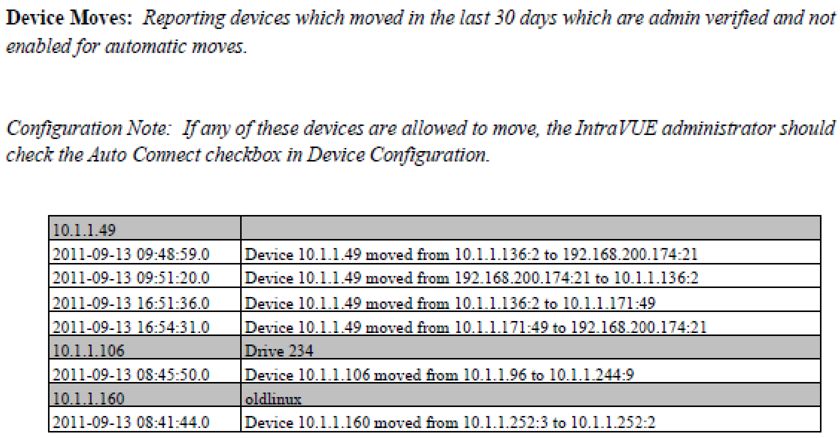


IntraVUE monitors the moves and provides a graphic indication if a device is moved. The picture on the left shows a Red Box to mark an unauthorized move and hovering over the connection shows the new port.

By selecting the Event Log for the device you can also get the day and time that the move was made. This may help identify details to avoid the move from happening in the future.

IntraVUE Diagnostics

Diagnostic Reports also provide a list and time of device moves. It can provide a very easy way for maintenance technicians to obtain a list of devices that have moved along with key data on the time and the original location.



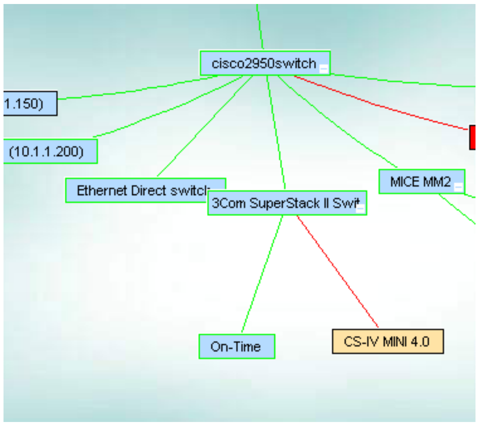
Device Moves: *Reporting devices which moved in the last 30 days which are admin verified and not enabled for automatic moves.*

Configuration Note: If any of these devices are allowed to move, the IntraVUE administrator should check the Auto Connect checkbox in Device Configuration.

10.1.1.49	
2011-09-13 09:48:59.0	Device 10.1.1.49 moved from 10.1.1.136:2 to 192.168.200.174:21
2011-09-13 09:51:20.0	Device 10.1.1.49 moved from 192.168.200.174:21 to 10.1.1.136:2
2011-09-13 16:51:36.0	Device 10.1.1.49 moved from 10.1.1.136:2 to 10.1.1.171:49
2011-09-13 16:54:31.0	Device 10.1.1.49 moved from 10.1.1.171:49 to 192.168.200.174:21
10.1.1.106	Drive 234
2011-09-13 08:45:50.0	Device 10.1.1.106 moved from 10.1.1.96 to 10.1.1.244:9
10.1.1.160	oldlinux
2011-09-13 08:41:44.0	Device 10.1.1.160 moved from 10.1.1.252:3 to 10.1.1.252:2

Foreign computers momentarily linking to the network

Security is important for any network. Although many automation systems are behind a firewall and have no access to the outside world, it does not mean they are fully protected. Outside suppliers can easily connect to the network. Even if the switches are locked in protected areas, one can use an Ethernet connection to an idle device to gain network access.



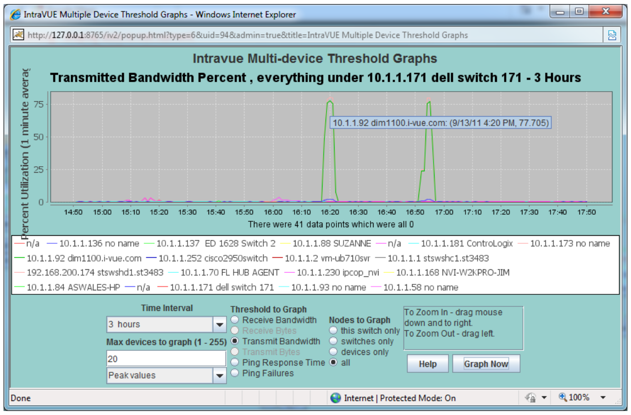
In many cases they may have the right to attach to the network but may inadvertently create a problem such as bandwidth problems when uploading a program or configuring a device. In some cases the foreign computer may only be on the network for a short time. Trying to identify an issue caused with the device now disconnected can be difficult.

IntraVUE identifies new devices with a tan colored box which is differentiated from the admin verified blue colored boxes. If the device is still connected to the network the line to the device would be green. A red line will indicate that the device is no longer communicating on the network. Clicking on the Event Log will provide details on the time the initial connection was made and if the device was moved to different locations in the network. If the device created traffic that exceeded the default presets it will also be logged and date stamped.

IntraVUE Diagnostics

Large File transfers between devices

Large transfers between devices could affect network performance by overloading switch traffic. These transfers may occur for a few minutes and disrupt other applications. Disruptions can be seen as a slowdown in communications or can actually lock up devices. As more devices are connected and use the network for management and configuration as well as Enterprise system gather reporting data the traffic flow can be unpredictable.


IntraVUE Multiple Device Threshold Graphs - Windows Internet Explorer
http://127.0.0.1:8765/iv2/popup.html?type=6&uid=94&admin=true&title=IntraVUE Multiple Device Threshold Graphs
Intravue Multi-device Threshold Graphs
Transmitted Bandwidth Percent , everything under 10.1.1.171 dell switch 171 - 3 Hours
Percent Utilization (1 minute averag
75
50
25
0
10.1.1.92 dim1100.i-vue.com: (9/13/11 4:20 PM, 77.705)
14:50
15:00
15:10
15:20
15:30
15:40
15:50
16:00
16:10
16:20
16:30
16:40
16:50
17:00
17:10
17:20
17:30
17:40
17:50
There were 41 data points which were all 0
n/a
10.1.1.136 no name
10.1.1.137 ED 1628 Switch 2
10.1.1.88 SUZANNE
n/a
10.1.1.181 ControLogix
10.1.1.173 no name
10.1.1.92 dim1100.i-vue.com
10.1.1.252 cisco2950switch
10.1.1.2 vm-ub710svr
10.1.1.1 stswshc1.st3483
192.168.200.174 stswshd1.st3483
10.1.1.70 FL HUB AGENT
10.1.1.230 ipcop_nvi
10.1.1.168 NVI-W2KPRO-JIM
10.1.1.84 ASWALES-HP
n/a
10.1.1.171 dell switch 171
10.1.1.93 no name
10.1.1.58 no name
Help
Graph Now
Done
Internet | Protected Mode: On
100%

Time Interval: 3 hours

Max devices to graph (1 - 255): 20

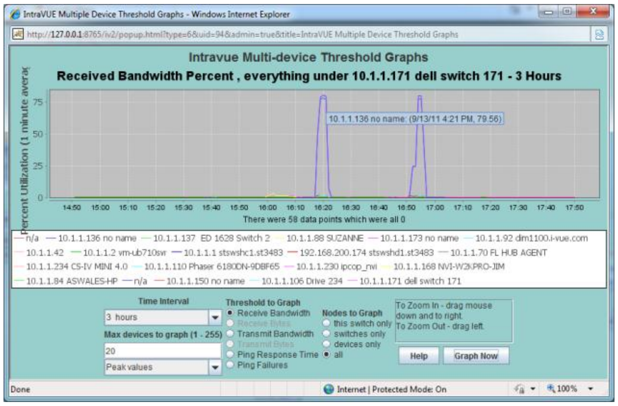
Peak values

Threshold to Graph: ○ Receive Bandwidth ○ Receive Bytes ● Transmit Bandwidth ○ Transmit Bytes ○ Ping Response Time ○ Ping Failures

Nodes to Graph: ○ this switch only ○ switches only ○ devices only ● all

To Zoom In - drag mouse down and to right.
To Zoom Out - drag left.

IntraVUE can provide specific details on the interaction hours after the event occurred. Many times there is no one immediately available to determine the source of the issue. The recording capability of IntraVUE can provide a time based view of the transmission and receiving of large amounts of data. In the two pictures one can see that there was a transfer between two devices that occurred at two separate times in the graph.


IntraVUE Multiple Device Threshold Graphs - Windows Internet Explorer
http://127.0.0.1:8765/iv2/popup.html?type=6&uid=94&admin=true&title=IntraVUE Multiple Device Threshold Graphs
Intravue Multi-device Threshold Graphs
Received Bandwidth Percent , everything under 10.1.1.171 dell switch 171 - 3 Hours
Percent Utilization (1 minute averag
75
50
25
0
10.1.1.136 no name: (9/13/11 4:21 PM, 79.56)
14:50
15:00
15:10
15:20
15:30
15:40
15:50
16:00
16:10
16:20
16:30
16:40
16:50
17:00
17:10
17:20
17:30
17:40
17:50
There were 58 data points which were all 0
n/a
10.1.1.136 no name
10.1.1.137 ED 1628 Switch 2
10.1.1.88 SUZANNE
10.1.1.173 no name
10.1.1.92 dim1100.i-vue.com
10.1.1.42
10.1.1.2 vm-ub710svr
10.1.1.1 stswshc1.st3483
192.168.200.174 stswshd1.st3483
10.1.1.70 FL HUB AGENT
10.1.1.234 CS-IV MINI 4.0
10.1.1.110 Phaser 6180DN-9DBF65
10.1.1.230 ipcop_nvi
10.1.1.168 NVI-W2KPRO-JIM
10.1.1.84 ASWALES-HP
n/a
10.1.1.150 no name
10.1.1.106 Drive 234
10.1.1.171 dell switch 171
Help
Graph Now
Done
Internet | Protected Mode: On
100%

Time Interval: 3 hours

Max devices to graph (1 - 255): 20

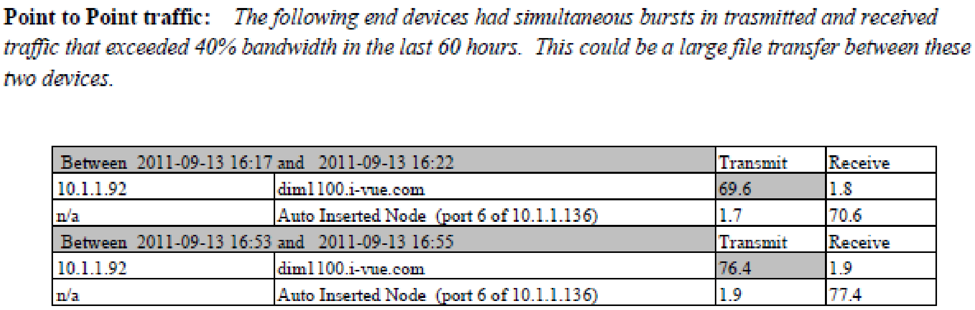
Peak values

Threshold to Graph: ● Receive Bandwidth ○ Receive Bytes ○ Transmit Bandwidth ○ Transmit Bytes ○ Ping Response Time ○ Ping Failures

Nodes to Graph: ○ this switch only ○ switches only ○ devices only ● all

To Zoom In - drag mouse down and to right.
To Zoom Out - drag left.

This data is also provided in the Diagnostic report so that the details are quickly identified without having to analyze and charts.



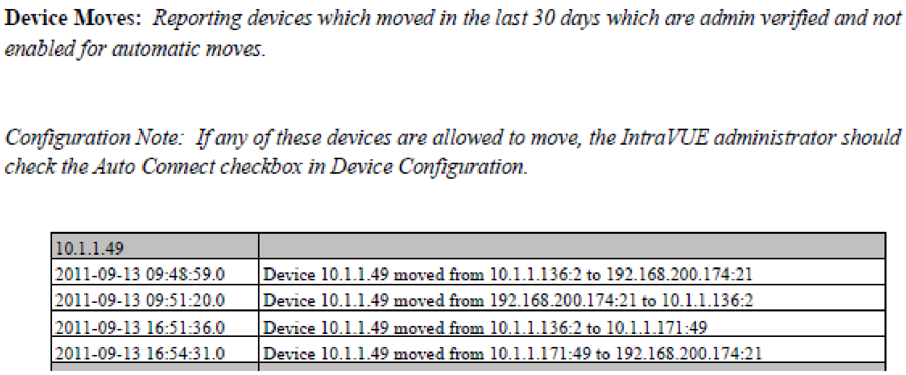
Point to Point traffic: *The following end devices had simultaneous bursts in trasmitted and received traffic that exceeded 40% bandwidth in the last 60 hours. This could be a large file transfer between these two devices.*

Between 2011-09-13 16:17 and 2011-09-13 16:22		Transmit	Receive
10.1.1.92	dim1100.i-vue.com	69.6	1.8
n/a	Auto Inserted Node (port 6 of 10.1.1.136)	1.7	70.6
Between 2011-09-13 16:53 and 2011-09-13 16:55		Transmit	Receive
10.1.1.92	dim1100.i-vue.com	76.4	1.9
n/a	Auto Inserted Node (port 6 of 10.1.1.136)	1.9	77.4

IntraVUE Diagnostics

Bad RSTP, Ring Switches, or accidental cable loops

IntraVUE continually communicates to the managed switches obtaining details how the switches are seeing the location of the devices. The communications occurs once a minute in which data from the switches Bridge MIB is accessed. This information is used to provide an accurate mapping of the interconnections of the network. IntraVUE is not a wiring diagram (however in most simple cases it represents the actual wiring) but represents what port the switch will use to send traffic to a specific device. This is the heart of the mapping capability of IntraVUE which also contains many rules and exceptions to deal with more complex architectures.



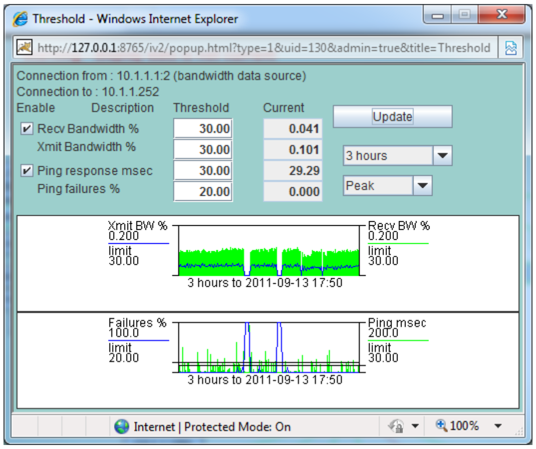
Device Moves: *Reporting devices which moved in the last 30 days which are admin verified and not enabled for automatic moves.*

Configuration Note: If any of these devices are allowed to move, the IntraVUE administrator should check the Auto Connect checkbox in Device Configuration.

10.1.1.49	
2011-09-13 09:48:59.0	Device 10.1.1.49 moved from 10.1.1.136:2 to 192.168.200.174:21
2011-09-13 09:51:20.0	Device 10.1.1.49 moved from 192.168.200.174:21 to 10.1.1.136:2
2011-09-13 16:51:36.0	Device 10.1.1.49 moved from 10.1.1.136:2 to 10.1.1.171:49
2011-09-13 16:54:31.0	Device 10.1.1.49 moved from 10.1.1.171:49 to 192.168.200.174:21

Occasionally the ability to have a single and consistent path for the switch can be interrupted. This can be caucused by a number of issues such as a loop back wiring, momentary link loses on a RSTP and Ring, or the switch being confused by MAC addresses that are too close in number. In these cases the IntraVUE may oscillate between to links or report MAC addresses on two different ports. These disturbances will be logged in the event log and may also be seen as the network changing in the main IntraVUE display. In this the IntraVUE is trying to accurately represent the network that is constantly changing.

Resetting Switch



Threshold - Windows Internet Explorer

http://127.0.0.1:8765/iv2/popup.html?type=1&uid=130&admin=true&title=Threshold

Connection from : 10.1.1.1:2 (bandwidth data source)
Connection to : 10.1.1.252

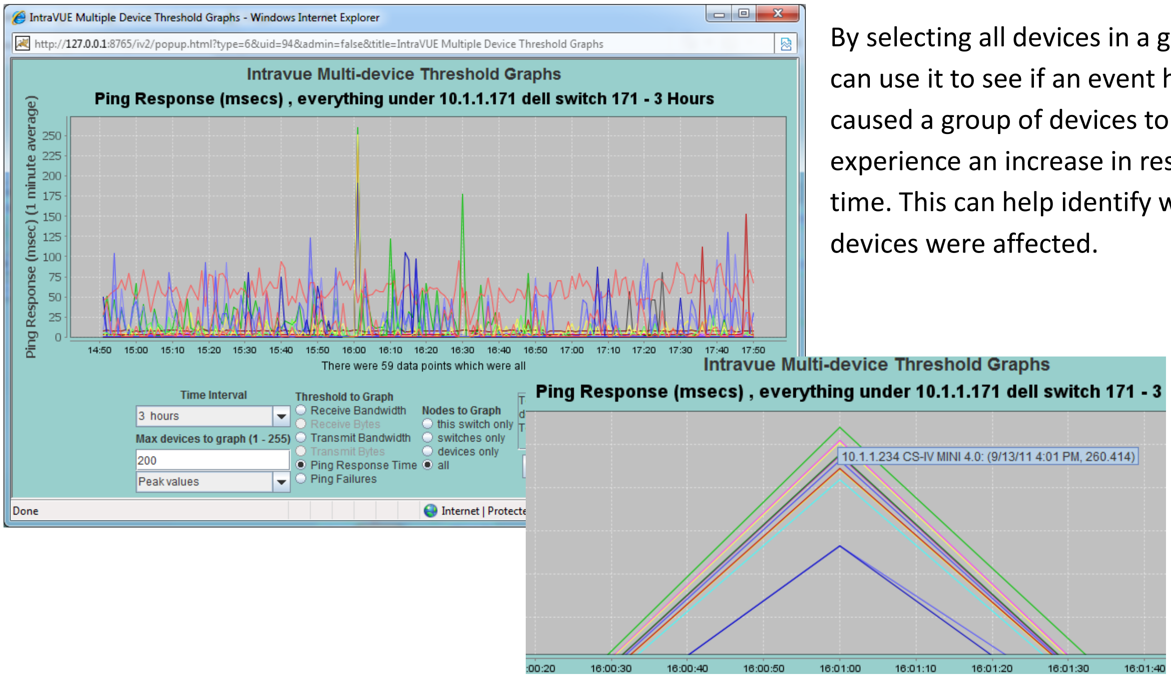
Enable	Description	Threshold	Current
☑	Recv Bandwidth %	30.00	0.041
	Xmit Bandwidth %	30.00	0.101
☑	Ping response msec	30.00	29.29
	Ping failures %	20.00	0.000

It is important to identify if a problem is application or network related. In one case a switch was having difficulty and doing a periodic reset. This is not uncommon with older switches. Many are configured to reset if their cash memory reach certain levels. Others may reset based on a poor power connection. Whatever the case the reset may create a momentary disruption in data transmission.

IntraVUE trends the transmitted and receive data on a timeline and below trend the ping response time and ping failure percentages below. This graphing can provide graphic evidence of the drop off of communications at the same time the ping failures go to 100%. The time basis also provides some clues to research to determining what may be happening with the switch at that time.

Overloaded or misbehaving devices

Automation networks contain many devices from several different manufactures. This diversity coupled with the ages of some of the equipment will mean at some point devices will start to have problems. One method to determine if a device is starting to have problems is a delay in the ping response time. By measuring the response time continually IntraVUE can have a means to determine if there are any relative issues that may be represented as a change in normal response times.



IntraVUE Multiple Device Threshold Graphs - Windows Internet Explorer

http://127.0.0.1:8765/iv2/popup.html?type=6&uid=94&admin=false&title=IntraVUE Multiple Device Threshold Graphs

Intravue Multi-device Threshold Graphs

Ping Response (msecs) , everything under 10.1.1.171 dell switch 171 - 3 Hours

There were 59 data points which were all

Time Interval: 3 hours

Max devices to graph (1 - 255): 200

Peak values

Threshold to Graph
○ Receive Bandwidth
○ Receive Bytes
○ Transmit Bandwidth
○ Transmit Bytes
● Ping Response Time
○ Ping Failures

Nodes to Graph
○ this switch only
○ switches only
○ devices only
● all

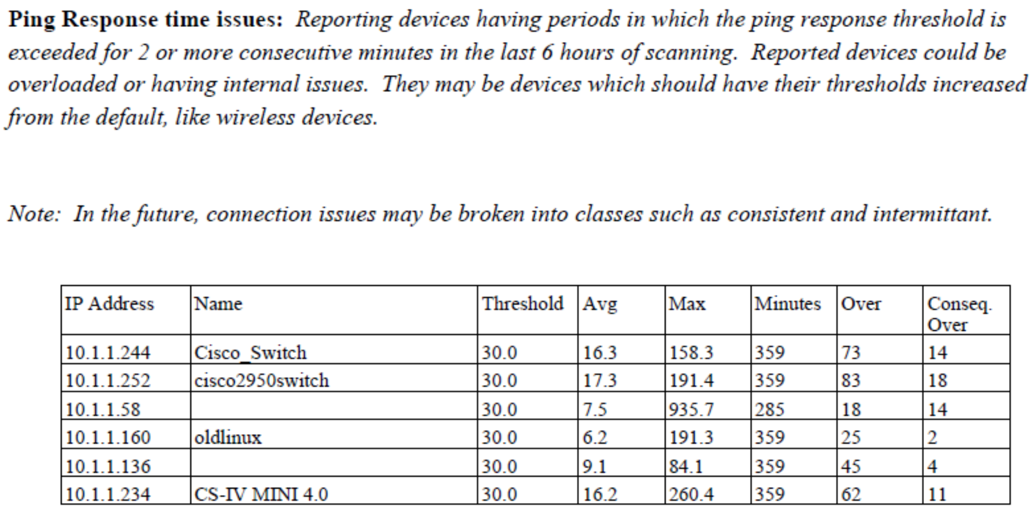
Done

Intravue Multi-device Threshold Graphs

Ping Response (msecs) , everything under 10.1.1.171 dell switch 171 - 3

10.1.1.234 CS-IV MINI 4.0: (9/13/11 4:01 PM, 260.414)

By selecting all devices in a graph you can use it to see if an event has caused a group of devices to experience an increase in response time. This can help identify what devices were affected.



Ping Response time issues: *Reporting devices having periods in which the ping response threshold is exceeded for 2 or more consecutive minutes in the last 6 hours of scanning. Reported devices could be overloaded or having internal issues. They may be devices which should have their thresholds increased from the default, like wireless devices.*

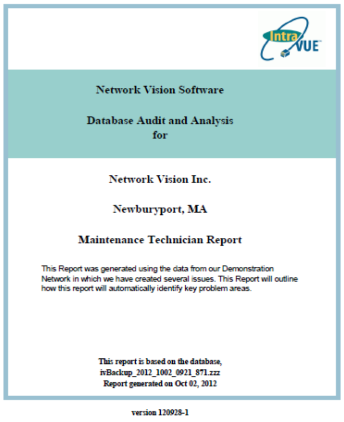
Note: In the future, connection issues may be broken into classes such as consistent and intermittant.

IP Address	Name	Threshold	Avg	Max	Minutes	Over	Conseq. Over
10.1.1.244	Cisco_Switch	30.0	16.3	158.3	359	73	14
10.1.1.252	cisco2950switch	30.0	17.3	191.4	359	83	18
10.1.1.58		30.0	7.5	935.7	285	18	14
10.1.1.160	oldlinux	30.0	6.2	191.3	359	25	2
10.1.1.136		30.0	9.1	84.1	359	45	4
10.1.1.234	CS-IV MINI 4.0	30.0	16.2	260.4	359	62	11

IntraVUE Diagnostics

The IntraVUE solution uses the data being collected for a variety of methods of interacting with individuals. Support of the automation networks may be shared between maintenance technicians, control engineers, and IT or network professionals. Each may have a different level of skill and interest. IntraVUE provides a variety of methods as a means to focus on the issues relating to each and delivers information in a variety of forms.

Basic Diagnostic Reports.



Network Vision Software

Database Audit and Analysis
for

Network Vision Inc.

Newburyport, MA

Maintenance Technician Report

This Report was generated using the data from our Demonstration Network in which we have created several issues. This Report will outline how this report will automatically identify key problem areas.

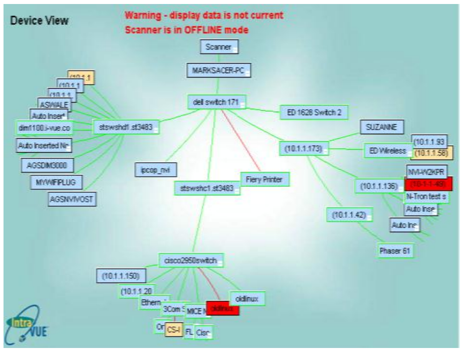
This report is based on the database,
ivBackup_2012_1002_0921_871.zzz
Report generated on Oct 02, 2012

version 120928-1

This has been referenced in the above as a way to provide analytical results based on our methodology. There will be a variety of reports to match the intention of the user. Visit http://www.intravue.net for more details.

- **Maintenance reports** will provide analysis of the issues occurring on the network
- **Asset Reports** will provide a spreadsheet with the key data such as device details and switch port location.
- **Configuration Reports** will help with the configuration of the IntraVUE system

Live IntraVUE Screen

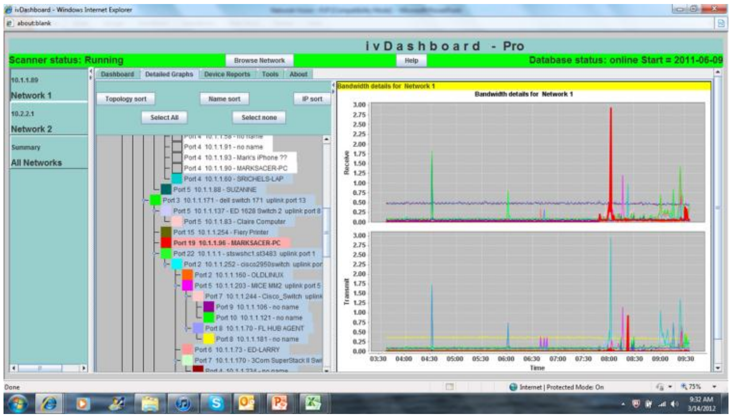


Warning - display data is not current
Scanner is in OFFLINE mode

IntraVUE provides a live animated graphical view that can be view from any computer browsing to the IntraVUE system. IntraVUE provides links to pop up windows that have been review in the above material.

This view is used by maintenance technicians and control engineers to quickly identify and resolve basic problems.

IntraVUE Dashboard

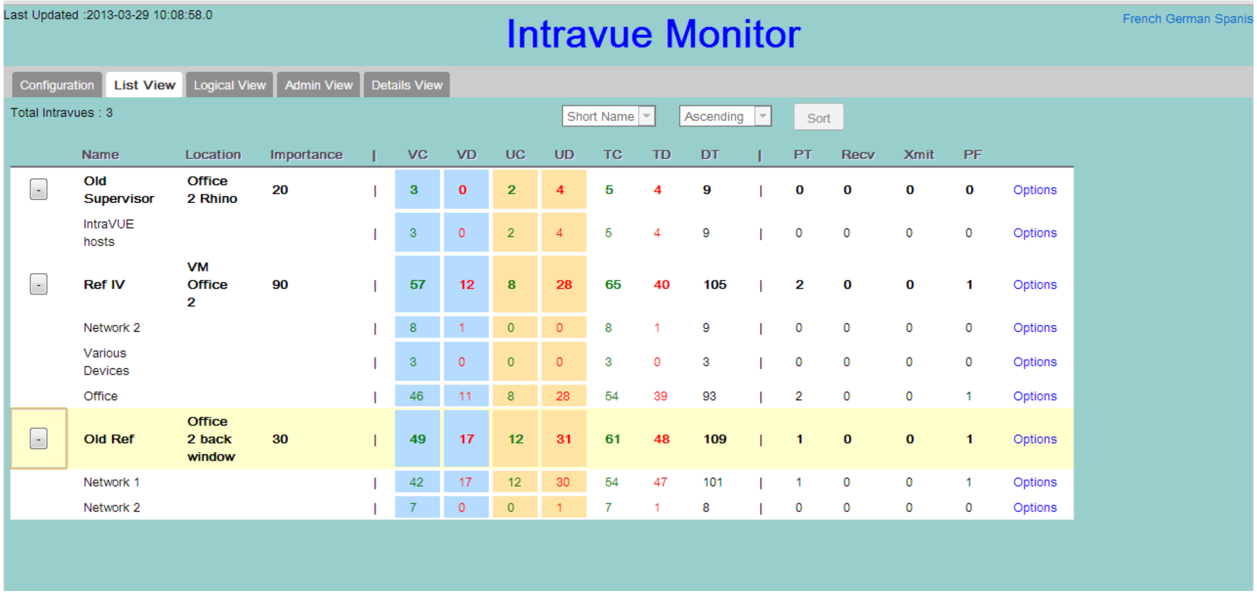


ivDashboard - Windows Internet Explorer
about:blank
ivDashboard - Pro
Scanner status: Running
Browse Network
Help
Database status: online Start = 2011-06-09
10.1.1.89
Network 1
10.2.2.1
Network 2
Summary
All Networks
Dashboard
Detailed Graphs
Device Reports
Tools
About
Topology sort
Name sort
IP sort
Select All
Select none
Port 4 10.1.1.91 - no name
Port 4 10.1.1.93 - Mark's iPhone ??
Port 4 10.1.1.90 - MARKSACER-PC
Port 4 10.1.1.60 - SRICHELS-LAP
Port 5 10.1.1.88 - SUZANNE
Port 3 10.1.1.171 - dell switch 171 uplink port 13
Port 5 10.1.1.137 - ED 1628 Switch 2 uplink port 8
Port 5 10.1.1.83 - Claire Computer
Port 15 10.1.1.254 - Fiery Printer
Port 19 10.1.1.96 - MARKSACER-PC
Port 22 10.1.1.1 - stswshc1.st3483 uplink port 1
Port 2 10.1.1.252 - cisco2950switch uplink por
Port 2 10.1.1.160 - OLDLINUX
Port 5 10.1.1.203 - MICE MM2 uplink port 5
Port 7 10.1.1.244 - Cisco_Switch uplink
Port 9 10.1.1.106 - no name
Port 10 10.1.1.121 - no name
Port 8 10.1.1.70 - FL HUB AGENT
Port 8 10.1.1.181 - no name
Port 6 10.1.1.73 - ED-LARRY
Port 7 10.1.1.170 - 3Com SuperStack II Swi
Bandwidth details for Network 1
Receive
Transmit
3.00
2.75
2.50
2.25
2.00
1.75
1.50
1.25
1.00
0.75
0.50
0.25
0.00
03:30
04:00
04:30
05:00
05:30
06:00
06:30
07:00
07:30
08:00
08:30
09:00
09:30
Time
Done
Internet | Protected Mode: On
75%
9:32 AM
3/14/2012

The IntraVUE Dashboard provide more experienced users with a way to associate the data collected in ways to help better review complex issues. It allows greater association of the devices with the switches as well as the inter relationships of the networks. The Dashboard is used by Control engineers and Manufacturing IT people.

IntraVUE Diagnostics

IntraVUE Supervisor



Last Updated :2013-03-29 10:08:58.0

Intravue Monitor

Total Intravues : 3

	Name	Location	Importance	|	VC	VD	UC	UD	TC	TD	DT	|	PT	Recv	Xmit	PF	
-	**Old Supervisor**	**Office 2 Rhino**	**20**	|	**3**	**0**	**2**	**4**	**5**	**4**	**9**	|	**0**	**0**	**0**	**0**	Options
	IntraVUE hosts			|	3	0	2	4	5	4	9	|	0	0	0	0	Options
-	**Ref IV**	**VM Office 2**	**90**	|	**57**	**12**	**8**	**28**	**65**	**40**	**105**	|	**2**	**0**	**0**	**1**	Options
	Network 2			|	8	1	0	0	8	1	9	|	0	0	0	0	Options
	Various Devices			|	3	0	0	0	3	0	3	|	0	0	0	0	Options
	Office			|	46	11	8	28	54	39	93	|	2	0	0	1	Options
-	**Old Ref**	**Office 2 back window**	**30**	|	**49**	**17**	**12**	**31**	**61**	**48**	**109**	|	**1**	**0**	**0**	**1**	Options
	Network 1			|	42	17	12	30	54	47	101	|	1	0	0	1	Options
	Network 2			|	7	0	0	1	7	1	8	|	0	0	0	0	Options

The IntraVUE Supervisor is used in large installations where many distributed IntraVUE systems are deployed. This can be in either a single large installation or a central support group supporting many different plants. The Supervisor monitors not only the health of the networks but also of the IntraVUE systems. It provides the ability of a single individual to oversee hundreds of IntraVUE systems and potentially thousands of networks easily.

I hope that this document provides good insight into the full capabilities of the powerful and scalable diagnostic tool.

For more information or a demonstration please contact Network Vision Software at www.intravue.net

Network Vision Software

44 Merrimac St.

Newburyport, MA 01950

+1 978 499-7800

www.intravue.net